IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

FELIX GONZALEZ, individually and on behalf of all others similarly situated, Plaintiff, v. AMERICAN FAMILY CARE, LLC, Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Felix Gonzalez ("Plaintiff"), individually and on behalf of all others similarly situated against Defendant American Family Care, LLC ("Defendant"). Plaintiff brings this action based on personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF ACTION

1. This is a class action lawsuit brought on behalf of all persons who have visited the website www.afcurgentcare.com (the "Website") and booked an appointment for an urgent care medical appointment.

2. When booking medical services online, patient privacy is crucial. Patients expect, as they should, that their private information will be held in confidence and not shared with third parties. The sensitive nature of information related to emergency medical services amplifies the need for privacy during online bookings, as these appointments often involve sensitive details of a patient's health.

3. Defendant owns and operates the Website, where patients can book medical services at one of its brick-and-mortar urgent care medical facilities.

4. Defendant offers a wide range of medical services to its patients, including urgent care, primary care, lab testing, physical exams, vaccinations, and x-rays.[1]

5. Defendant is a covered entity under HIPAA and must comply with its rules and regulations, including those regarding patient privacy.

6. Despite its ethical and legal duties as a medical provider, and unbeknownst to Plaintiff and members of the putative class, Defendant discloses its patients' protected health information ("PHI") to third parties, including Google LLC ("Google"), for targeted advertising purposes. Plaintiff brings this action for legal and equitable remedies resulting from Defendant's illegal actions.

THE PARTIES

7. At all relevant times, Plaintiff was a resident of Howard Beach, New York. Plaintiff has been a patient of American Family Care since 2025. On or around March 2025, Plaintiff scheduled an urgent care appointment for medical services through Defendant's Website. This appointment was scheduled for March 8, 2025, at Defendant's Howard Beach location.[2]

8. Unbeknownst to Plaintiff, Defendant disclosed his PHI—including the fact that he was booking an appointment for medical services and the specific medical services sought—to Google for targeted advertising purposes. Defendant also disclosed sufficient personally identifiable information ("PII") for Google to identify Plaintiff as the specific individual booking his medical appointment, as described more thoroughly below.

[1] https://www.afcurgentcare.com/patient-services/

[2] In order to protect Plaintiff's privacy, the type of treatment he sought has been omitted from this Complaint.

9. After booking an appointment on the AFC Urgent Care Website, Plaintiff began receiving targeted advertisements for similar products and services. Plaintiff would not have booked an appointment on the Website if he knew the Defendant was violating his privacy by sharing his PHI with unknown third parties.

10. At all relevant times Plaintiff has maintained a Gmail account. When registering for his Gmail account, Google required that she provide his full legal name, date of birth, and gender. Every time Plaintiff accesses his Gmail account, Google collects information related to his IP address and electronic device (e.g. browser, operating system, screen resolution, etc.) and stores it in a profile maintained by Google for targeted advertising purposes. Google also utilizes other features, such as generating specific User IDs, to track its users across web browsing sessions for identification purposes, as detailed below. Google utilizes all of these tracking features in order to build robust consumer profiles it can then leverage for targeted advertising purposes.

11. American Family Care, LLC is an Alabama corporation with its principal place of business in Brimingham, Alabama. Defendant owns and operates a professional network of brick-and-mortar medical clinics that specialize in urgent care medical services. Defendant also develops, owns, and operates the Website, which is used by its patients throughout the United States, to book appointments for medical services. Defendant chose to embed Google's tracking technology on its Website, whereby it intercepted and disclosed the confidential medical information of its patients to Google for targeted advertising purposes. Defendant did this without consent or authorization from its patients.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from at least one defendant.

13. This Court has personal jurisdiction over the Defendant because Defendant conducts substantial business within this District.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

A. Health-Related Information is Sensitive and Confidential

15. Defendant intercepted and disclosed to Google, one of the largest data and technology companies in the world, information that is sensitive, confidential, and personally identifiable.

16. Defendant operates a network of urgent care facilities throughout the United States. Defendant also maintains its Website, where it encourages its patients to schedule medical appointments.

17. Under federal law, a healthcare provider may not disclose personally identifiable information ("PII") or protected health information ("PHI") without the patient's express written

authorization.[3] In this case, PHI includes, but is not necessarily limited to, information pertaining to medical services.

18. The United States Department of Health and Human Services ("HHS") has established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare providers owe to their patients. "The Rule requires appropriate safeguards to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization."[4]

19. A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[5]

20. The statute states that an entity "shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity…and the individual obtained or disclosed such information without authorization." *Id*.

21. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant because they are knowingly disclosing individually identifiable health information relating to its patients.

22. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that

[3] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

[4] U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[5] 42 U.S.C. § 1320d-6.

Defendant created, received, maintained and transmitted in violation of 45 C.F.R. Section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.R.F. Section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R. Section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);

e. Failing to protect against reasonably anticipated uses of disclosures of electronic PHI not permitted under privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. Section 164.306(a)(3); and

f. Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. Section 164.530(c).

23. Health care organizations regulated under HIPAA, like Defendant, may use third-party tracking tools in a limited way to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to vendors (as shown below). As explained by a statement published by the HHS:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would

> result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures**.[6]

24. The Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**[7]

25. Plaintiff and Class members face exactly the risks about which the government expresses concern. Defendant's unlawful conduct resulted in third parties intercepting information regarding Plaintiff and Class members' medical services appointments and treatments.

26. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or **dates of appointments**, as well as **an individual's IP address** or geographic location, medical

[6] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[7] *Id.* (emphasis added).

device IDs, **or any unique identifying code**.[8]

27. Crucially, the Bulletin continues:

> **All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI**, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, **such as IP address** or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus **relates to the individual's past, present, or future health or health care** or payment for care.[9]

28. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.
>
> "When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

[8] *Id.* (emphasis added).

[9] *Id.* (emphasis added).

> "Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."
>
> The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.
>
> In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, **medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment**.[10]

29. The FTC is unequivocal in its stance. The FTC has specifically informed healthcare companies, like Defendant, that they should not use tracking technologies to collect sensitive health information and disclose it to third party advertising platforms without informed consent:

> The FTC Act prohibits companies and individuals from engaging in unfair or deceptive acts or practices in or affecting commerce. This means you must ensure your health data practices aren't substantially injuring consumers, including by invading their privacy.

[10] Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking (emphasis added).

> For instance, *BetterHelp*, *GoodRx*, and *Premom* make clear that disclosing consumers' health information for advertising without their affirmative express consent may be an unfair practice.
>
> [I]f you use behind-the-scenes tracking technologies that share consumers' sensitive health data in contradiction of your privacy promises, that's a violation of the FTC Act.[11]

30. Therefore, Defendant's conduct, as described herein, is directly contrary to federal law and the clear pronouncements by the FTC and HHS.

B. Google's Advertising Technology

31. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each device (such as a computer, tablet, laptop, or smartphone) accesses web content through a web browser (e.g. Chrome, Safari, Edge, etc.).

32. Every website is hosted by a computer server that holds the website's contents and through which the entity in charge of the website exchanges communications with the consumer's device via web browsers.

33. Web communications consist of HTTP Requests and HTTP Responses and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- HTTP Request: an electronic communication sent from a device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

- Cookies: a small text file that can be used to store information on the device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from devices to the host server. Some cookies are "third-party

[11] https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach

cookies," which means they can store and communicate data when visiting one website to an entirely different website.

- HTTP Response: an electronic communication that is sent as a reply to the device's web browser from the host server in response to a HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

34. A consumers' HTTP Request essentially asks the Website to retrieve certain information (such as appointment booking information), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the consumer's screen as they navigate the Website).

35. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

36. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. The tracking technologies embedded on the Website by Defendant constitute Source Code and function is a substantially similar way.

37. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over $1 trillion dollars. Google fancies itself a "tech" company, but Google, at its core, is an advertising company.

38. Google "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," generating "revenues primarily by delivering both performance advertising and brand advertising."[12] In 2020, Google generated $146.9 billion in advertising

[12] ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.

revenue, which amounted to more than 80 percent of Google's total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Figure 1:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$257.6 billion	$209.5	81.33%
2020	$182.5 billion	$146.9 billion	80.49%
2019	$161.9 billion	$134.8 billion	83.29%
2018	$136.8 billion	$116.5 billion	85.12%

39. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google's SDK and pixel integrate with Google's advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google's ad network and products increasing Google's overall ad revenue. Products like Google's SDK and its tracking pixel also improve the company's advertising network and capabilities by providing more wholesome profiles and data points on individuals.

40. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

41. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a

persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices."

42. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

43. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a $62.6 billion increase in advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

44. Google touts Google Analytics as a marketing platform that offers "a complete understanding of your customers across devices and platforms."[13] It allows companies and advertisers that utilize it to "understand how your customers interact across your sites and apps, throughout their entire lifestyle," "uncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data," "take action to optimize marketing performance with integrations across Google's advertising and publisher tools," and "quickly analyze your data and collaborate with an easy-to-use interface and shareable reports."[14]

45. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site. This code immediately intercepts a user's interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or

[13] *Analytics*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Jan. 10, 2023).

[14] *Id.*

patient) is using to access a website. The device information intercepted by Google includes the patient's operating system, operating system version, browser, language, and screen resolution.

46. In other words, when interacting with the Website, an HTTP Request is sent to Defendant's server, and that server sends an HTTP Response including the Markup that displays the website visible to the patient and Source Code, including Google's tracking technologies.

47. Thus, Defendant is essentially handing their patients a tapped device, and once the webpage is loaded onto the patient's browser, the software-based wiretap is quietly waiting for private communications on the Website to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third parties like Google.

48. Once Google's software code collects the data intercepted from the Website, it packages the information and sends it to Google Analytics for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

49. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

50. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

51. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the medical services being received by the patient. Google also received additional PII, including the patients' IP address, device information, and User-IDs.

52. For example, the Website utilizes Google's "cid" or "Client ID" function to identify users as they navigate the Website.

53. In addition to User-IDs, upon receiving information from the Website, Google also utilizes a "browser-fingerprint" to personally identify consumers. A browser-fingerprint is information collected about a computing device that is used to identify the specific device.

54. These browser-fingerprints are used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data.

55. As Google explained, "[w]ith fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[15]

56. The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it

[15] https://www.blog.google/products/chrome/building-a-more-private-web/

employs much more subtle techniques.[16] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.

57. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[17]

58. Browser-fingerprints are personal identifiers. Tracking technologies, like the ones developed by Google and utilized on the Website, can collect browser-fingerprints from website visitors.

59. As enabled by Defendant, Google collects vast quantities of consumer data through its tracking technology.

60. Due to the vast network of consumer information held by Google, it is able to match the IP addresses, device information, and User-IDs it intercepts and link such information to an individual's specific identity.

61. Google then utilizes such information for its own purposes, such as targeted advertising.

C. Defendant Violates the Privacy Rights of Its Patients

42. Defendant allows its patients to book appointments for medical services through its Website.

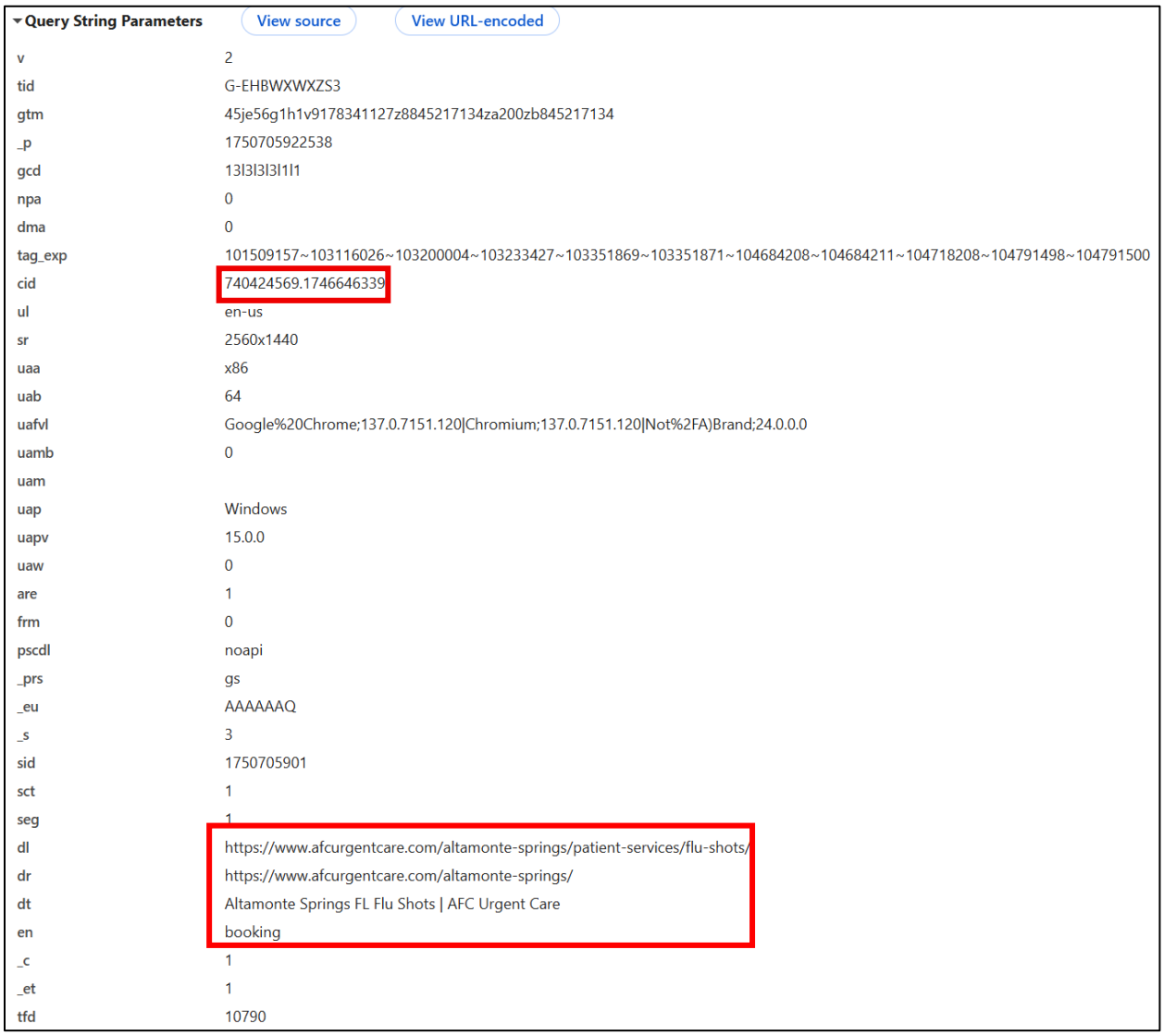
43. Unbeknownst to its patients, Defendant embedded Google's tracking technologies onto the Website, through which Defendant is able to intercept and disclose its patients' confidential communications to Google.

[16] https://www.pixelprivacy.com/resources/browser-fingerprinting/

[17] https://ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

44. For example, when a patient books an appointment for a flu shot at Defendant's Altamonte Springs location, Defendant unlawfully discloses such information to Google.

Figure 2:



Query String Parameters | View source | View URL-encoded

v	2
tid	G-EHBWXWXZS3
gtm	45je56g1h1v9178341127z8845217134za200zb845217134
_p	1750705922538
gcd	13l3l3l3l1l1
npa	0
dma	0
tag_exp	101509157~103116026~103200004~103233427~103351869~103351871~104684208~104684211~104718208~104791498~104791500
cid	740424569.1746646339
ul	en-us
sr	2560x1440
uaa	x86
uab	64
uafvl	Google%20Chrome;137.0.7151.120|Chromium;137.0.7151.120|Not%2FA)Brand;24.0.0.0
uamb	0
uam	
uap	Windows
uapv	15.0.0
uaw	0
are	1
frm	0
pscdl	noapi
_prs	gs
_eu	AAAAAAQ
_s	3
sid	1750705901
sct	1
seg	1
dl	https://www.afcurgentcare.com/altamonte-springs/patient-services/flu-shots/
dr	https://www.afcurgentcare.com/altamonte-springs/
dt	Altamonte Springs FL Flu Shots | AFC Urgent Care
en	booking
_c	1
_et	1
tfd	10790

45. Defendant further assists Google by disclosing the PII of its patients sufficient for Google to uncover their identities. In the HTTP communication displayed in Figure 2, the patient's IP address is inherently included in every network request. In addition to its patients' IP addresses, Defendant, through Google's tracking technologies, disclosed information about

their specific devices and User-IDs to Google, allowing Google to link such information to an individual's specific identity.

46. As shown above, Plaintiff's communications with Defendant were disclosed by Defendant to Google and/or intercepted in transit, in real time, via detailed URLs, which contain the medically sensitive and personally identifiable information entered into the Website.

47. Defendant also uses and causes the disclosure of data sufficient for Google to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual medical appointments.

48. Defendant sent these identifiers (e.g. cid, IP address, and device information) with each patient's "event" data.

49. Such event data includes the fact that a patient is seeking medical services, the location of the appointment, the reason for the visit, and their appointment status. *See* Figure 2.

50. When patients share their personal information with medical professionals, they expect this information to be kept confidential. Moreover, when consumers seek a specific service from medical professionals, they also expect this highly sensitive information to be kept confidential.

51. If patients knew that Defendant was sharing their personal information for targeted advertising purposes, they would have sought medical services with another company. Through the above-listed third party tracking services, which Defendant used via the software code installed, integrated and embedded into the Website, Defendant disclosed its patients' legally protected PII and PHI.

52. By installing, integrating and embedding the above-listed tracking technologies into the Website, Defendant aided and conspired with third parties to contemporaneously and

surreptitiously intercept the Website communications of Defendant's patients without the patients' consent.

53. Defendant engages in this deceptive conduct for its own profit at the expense of its patients' privacy. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violate federal and state law.

CLASS ACTION ALLEGATIONS

54. Plaintiff brings this action on behalf of all persons in the United States who booked an appointment on www.afcurgentcare.com (the "Class").

55. Excluded from the Class are Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendant has or had a controlling interest.

56. Plaintiff is a member of the Class he seeks to represent.

57. The Class is so numerous that joinder of all members is impracticable. Although Plaintiff does not yet know the exact size of the Class, it is believed that there are at least thousands of Class members.

58. The Class is ascertainable because the Class members can be identified by objective criteria – all individuals who booked an appointment on www.afcurgentcare.com. Individual notice can be provided to Class members "who can be identified through reasonable effort." Fed. R. Civ. P. 23(c)(2)(B).

59. There are numerous questions of law and fact common to the Class, which predominate over any individual actions or issues, including but not limited to:

A. Whether Defendant gave the Class members a reasonable expectation of privacy that their information was not being shared with third parties;

B. Whether Defendant's disclosure of information constitutes a violation of the claims asserted;

C. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

D. Whether Plaintiff and Class members have sustained damages as a result of Defendant's conduct and if so, what is the appropriate measure of damages or restitution.

60. Plaintiff's claims are typical of the claims of the members of the Class, as all members are similarly affected by Defendant's wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Class have sustained economic injury arising out of Defendant's violations of common and statutory law as alleged herein.

61. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained counsel competent and experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and his counsel.

62. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation

increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

63. Plaintiff reserves the right to revise his allegations and class definition based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1), *et seq.*

64. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

65. Plaintiff brings this claim on behalf of himself and members of the Class.

66. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

67. The ECPA protects both sending and the receipt of communications.

68. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

69. The transmission of Plaintiff's PII and PHI to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

70. The transmission of PII and PHI between Plaintiff and Class members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

71. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

72. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

73. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

74. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and Google used to track Plaintiff and Class members communications while they were navigating the Website;

b. Plaintiff's and Class members' browsers;

c. Plaintiff's and Class members' mobile devices;

d. Defendant's and Google's web and ad servers;

e. The plan Defendant and Google carried out to effectuate the tracking and

interception of Plaintiff's and Class members' communications while they were using a web browser to navigate the Website.

75. Plaintiff and Class members' interactions with Defendant's Website are electronic communications under the ECPA.

76. By utilizing and embedding the tracking technology provided by Google on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

77. Specifically, Defendant intercepted—in real time—Plaintiff's and Class members' electronic communications via the tracking technology provided by Google on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and PHI to third parties, such as Google.

78. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class members regarding PII and PHI, including their identities and information related to their medical services appointments. This confidential information is then monetized for targeted advertising purposes, among other things.

79. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

80. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, while knowing or having reason to know that the

information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

81. Defendant intentionally intercepted the contents of Plaintiff's and Class members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, HIPAA, among others.

82. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[18]

83. Plaintiff's information that Defendant disclosed to Google qualifies as IIHI, and Defendant violated Plaintiff's and Class members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the electronic communications to increase their profit margins. Defendant

[18] 42 U.S.C. § 1320d-6.

specifically used the tracking technology provided by Google to track and utilize Plaintiff's and Class members' PII and PHI for financial gain.

84. Defendant was not acting under the color of law to intercept Plaintiff's and Class members' wire or electronic communications.

85. Plaintiff and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class members' privacy. Plaintiff and Class members, all of whom are patients of Defendant, had a reasonable expectation that Defendant would not redirect their communications to Google without their knowledge or consent.

86. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq*.

87. As a result of each and every violation thereof, on behalf of himself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

COUNT II
Negligence

88. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

89. Plaintiff brings this claim on behalf of himself and members of the Class against Defendant.

90. Upon accepting, storing and controlling the PHI and PII of Plaintiff and the Class, Defendant owed—and continues to owe—a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive PHI and PII.

91. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PHI and PII from unauthorized disclosure.

92. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PHI and PII through their use of the tracking technology would result in unauthorized third parties—such as Google—gaining unlawful access to such information.

93. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' PHI and PII arose due to the special relationship that existed between Defendant and their patients, which is recognized by statute and common law.

94. Defendant separately had a duty under HIPAA privacy laws, which was enacted with the objective of protecting the confidentiality of patients' medical-related information and set forth the conditions under which such information can be used and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

95. Defendant had an additional, separate duty under the FTC Act to not disclose its patients' PII and PHI.

96. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PHI and PII. Defendant's misconduct included the failure to: (i) secure Plaintiff's and Class Members' Private Information; (ii) comply with industry-standard data security practices; (iii) implement adequate Website and event monitoring and (iv) implement

the systems, policies and procedures necessary to prevent unauthorized disclosures resulting from the use of the tracking technology implemented by Defendant.

97. As a direct result of Defendant's actions, including but not limited to the disclosure of Plaintiff's and Class Members' PHI and PII, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, and emotional distress.

98. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class Members' Private Information constituted (and continues to constitute) negligence at common law.

99. Plaintiff and the Class are entitled to recover damages in an amount to be determined at trial.

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

a. Determining that this action is a proper class action;

b. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class and naming Plaintiff's attorneys as Class Counsel to represent the Class;

c. For an order declaring that Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

e. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

g. For prejudgment interest on all amounts awarded;

h. For injunctive relief ordering Defendant to immediately cease its illegal conduct;

i. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and

j. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: July 10, 2025

Respectfully submitted,

By: */s/ Alec Leslie*

BURSOR & FISHER, P.A.
Alec M. Leslie
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

BURSOR & FISHER, P.A.
Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: sbeck@bursor.com

Attorneys for Plaintiff